

CLAIM AMENDMENTS

This listing of claims will replace all prior versions and listings of claims in the application.

1 1. (Currently Amended) A method of detecting denial of service (DoS) attacks in an
2 Internet accessible network having at least one proxy server incorporating a session
3 initiation protocol (SIP), said SIP including incoming INVITE messages that
4 request set-up of an Internet telephone call and outgoing 180 Ringing messages
5 that indicate ringing, the method comprising ~~the following steps:~~

6 aggregating said INVITE messages and said 180 Ringing messages for all
7 users on said Internet accessible network;

8 detecting an imbalance between a number of said INVITE and 180 Ringing
9 messages resulting from a DoS attack; and

10 providing an indication of ~~the~~ a presence of a current DoS attack on said
11 proxy server based on detection of said imbalance.

1 2. (Currently Amended) The method of claim 1,

2 wherein a number (H) of INVITE messages including credentials that are
3 sent from a user client in response to an authentication required message from the
4 proxy server, said credentials being information used by the proxy server to

authenticate the INVITE messages, are removed from ~~the-an~~ accounting before the
~~balance-inbalance~~ is tested such that when ~~the-an~~ equation:

$$\text{INV}_o [[\text{to}]] + \text{INV}_c - H = N_{180}$$

where INV_o is ~~the-a~~ number of INVITE messages without said credentials,

INV_c is ~~the-a~~ number of INVITE messages with said credentials, and

N_{180} is ~~the-a~~ number of said 180 Ringing messages,

is not true within a predetermined margin of error,

then the presence of ~~a-said current~~ DoS attack on the proxy server is indicated by

~~the-an inequality in said equation.~~

3. (Currently Amended) The method of claim 2, further ~~comprising-including~~
~~the following step:~~

~~causing said proxy server to maintain-creating~~ a call information table ~~at~~
~~said proxy server~~ for determining ~~the-a~~ value of H.

4. (Canceled)

5. (Currently Amended) A system for detecting denial of service (DoS) attacks
against session initiation protocol elements in ~~a-an~~ Internet accessible network
having at least one proxy server, said system comprising:

4 | means for aggregating ~~said-incoming~~ INVITE messages and ~~said-outgoing~~
5 | 180 Ringing messages for all users on said Internet accessible network; and

6 | means, within said proxy server, for determining if ~~the-a~~ number of ~~said~~
7 | INVITE messages including credentials (INV_c) sent to said proxy server from user
8 | clients in response to an authentication requirement exceeds a number of said 180
9 | Ringing messages that indicates a DoS attack, said credentials being information
10 | used by the proxy server to authenticate the INVITE messages.

1 | 6. (Currently Amended) A system for detecting denial of service (DoS) attacks
2 | in an Internet accessible network having at least one proxy server incorporating a
3 | session initiation protocol (SIP), said system comprising:

4 | means for aggregating ~~said-incoming~~ INVITE messages and ~~said-outgoing~~
5 | 180 Ringing messages for all users on said Internet accessible network; and

6 | means, within said proxy server, for detecting an imbalance between a
7 | number of said INVITE and said 180 Ringing messages, the imbalance indicating
8 | ~~the-a~~ presence of a current DoS attack on said proxy server.

1 | 7. (Previously Presented) The system of claim 5, wherein said means for
2 | determining creates a call-info table for use in tracking said INVITE messages.

1 8. (Currently Amended) The system of claim 6, wherein said means for
2 detecting creates a call-info table for use in tracking said INVITE messages.